McAfee Total Protection for Endpoint—Enterprise Edition

Complete endpoint security designed for medium to large enterprises

Providing a secure endpoint environment for your business can be complex. Sophisticated malware and a boundary free workplace make it easy for cybercriminals to steal information and devices. Users expect support for their preferred systems, including Macs and mobile devices, while regulations force increased safeguards for data and documented compliance. All the while, the growing number of security point products increases management costs and complicates response. McAfee® Total Protection for Endpoint—Enterprise Edition unites industry-leading endpoint security and data protection with centralized management for ironclad security that streamlines operations and eases compliance.

Key Points

- Ironclad protection for all endpoints
- Lower operational costs with centralized management
- Compliance made simple with standard templates

"NSS Labs created variants of the Operation Aurora attack and tested the anti-malware software to see which of the seven products stopped the exploits and malicious code payloads. Given the level of visibility of the attack and the time that has passed since its initial discovery, it was thought that most, if not all, of the products would cover the vulnerability. However, only one out of seven tested products correctly thwarted multiple exploits and payloads, demonstrating vulnerability-based protection (McAfee)."

—NSS Labs Finds Most Endpoint Security Products Lack "Vulnerability-Based Protection"
http://nsslabs.com/nss-labs-in-thenews/nss-labs-finds-most-endpointsecurity-products-lack-vulnerabilitybased-protection

SC MAGAZINE AWARDS 2010 WINNER
Honored in the U.S.

Best Anti-Malware Solution and
Best Enterprise Security Solution

Today's threat landscape hides an ever-changing stream of worms, spyware, Trojans, bots, rootkits, hackers, identity thieves, and targeted attacks. These threats affect users who expect to take work with them everywhere, but unknowingly jeopardize your network and systems when they return to the office. With stringent requirements to safeguard data as well as verify and report on regulatory compliance, the risks are higher than ever. Yet your budget requires you to be frugal.

You could patch together a collection of individual products, but you would never achieve the effectiveness and efficiency of McAfee Total Protection for Endpoint—Enterprise Edition. That's because we integrate technologies for coordinated, complete solutions that offer the best defenses against today's multivector threats. This integrated security delivers ironclad protection, for all your endpoints, including Windows, Mac, and Linux systems and mobile devices.

Seamless integration secures your systems and data against sophisticated malware, shielding your assets from bots and zero-day attacks. It protects even if the device is lost or stolen, and blocks noncompliant systems or unauthorized devices that may attempt to access your business-critical systems and sensitive data.

This combination of controls is ideal for sophisticated enterprises with users who expect freedom—as well as total protection from the risks their mobility and flexibility entail.

Management that lowers operational costs

For efficiency and comprehensive visibility across your security and compliance status, McAfee ePolicy Orchestrator® (ePO™) software provides a single, centralized, platform that manages security, enforces protection, and lowers the cost of security operations. Web-based for easy access anywhere, it provides intelligent security for quick and effective decisions and greater control.

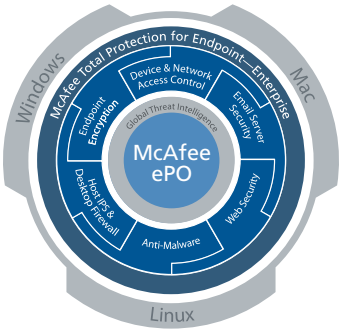
Correlate threats, attacks, and events from endpoint, network, and data security as well as compliance audits to improve the relevance and efficiency of security efforts and compliance reports. No other vendor can claim a single integrated management platform across all these security domains. McAfee ePolicy Orchestrator simplifies security management.

Persistent full-disk encryption

Comprehensive full-disk encryption for laptops and mobile devices prevents loss of sensitive data with lost or stolen equipment. Organizations can efficiently encrypt and decrypt devices at any time,

McAfee sets the industry standard

- Recognized for four straight years by Gartner as a leader in Endpoint Security and Mobile Data Protection
- First to manage broad range of security products including endpoint, network, data, web, and email security with one console
- First to deliver single agent and single console for endpoint security
- First product to have unified management platform for endpoint security and compliance management
- First product to manage both McAfee and third-party security products
- First to combine policy auditing and policy enforcement in a single engine
- First to combine endpoint security and data protection in one truly integrated suite



Ironclad protection for all your endpoints, including Windows, Mac, and Linux systems and mobile devices.

without interrupting users or system performance. Persistence helps enforce security policies and achieve regulatory compliance.

Comprehensive device management

To protect critical data from leaving your company through removable media, we give you tools to monitor and control data transfers from all desktops and laptops. You can control USB drives, iPods, and DVD use—regardless of where users and confidential data go, even when they leave the corporate network.

Zero-day protection and vulnerability shielding

Say goodbye to emergency patching. Host intrusion prevention patrols your endpoints against malware, blocks malicious code from hijacking an application, and provides automatically updated signatures that shield desktops and servers from attack while you implement and test patches on your schedule. Combined with our patented behavioral protection, which prevents buffer overflow attacks, you get the most advanced system vulnerability coverage on the market. McAfee has provided zero-day protection for ninety percent of critical Microsoft vulnerabilities.

Stateful desktop firewall

Control desktop applications that can access the network to stop network-borne attacks and downtime. You can deploy and manage firewall policies based on location to deliver complete protection and compliance with regulatory rules.

Efficient policy auditing and compliance

Agent-based policy auditing scans your endpoints and documents that all policies are up to date. Organizations can measure compliance to best practice policies—ISO 27001 and CoBIT—as well as to key industry regulations.

Advanced email virus and spam protection

Our solution scans your inbound and outbound emails for spam, inappropriate content, and harmful malware. Suspicious emails are quarantined to prevent evolving email threats from affecting your network and users. For extra assurance, a layer of anti-virus protects your email server and intercepts malware before it reaches user inboxes.

Proactive web security and content filtering

Many web threats are silent and invisible to web surfers. Help ensure compliance and reduce risk from web surfing by warning users about malicious websites before they visit. You can authorize and block website access, controlling users whether they are web surfing on or off the

Feature	Why You Need It
Single integrated management	McAfee ePolicy Orchestrator (ePO) provides instant visibility into security status and events and direct access to management for unified control of all your security and compliance tools
Encryption	Safeguards data and minimizes compliance issues with transparent on-the-fly encryption and strong access control
Device control	Lets you monitor and restrict data copied to removable storage devices and media to keep it from leaving company control
Host IPS and desktop firewall	Provides zero-day protection against new vulnerabilities, which reduces the urgency to patch existing systems, and controls desktop applications that can access the network to stop network-borne attacks and related downtime
Anti-malware	Blocks viruses, Trojans, worms, adware, spyware, and other potentially unwanted programs that steal confidential data and sabotage user productivity
Anti-spam	Helps eliminate spam, which can lead unsuspecting users to sites that distribute malware and phish for personal and financial data
Safe surf and search	Helps ensure compliance and reduce risk from web surfing by warning users about malicious websites before they visit and letting administrators authorize or block website access
Host web filtering	Controls users whether they are web surfing on or off the corporate network through content filtering and enforcement of website access by user and groups
Email server security	Protects your email server and intercepts malware before it reaches the user inbox
Network access control	Limits malware infections by preventing noncompliant systems from accessing the network
Policy auditing	Provides tightly integrated compliance reporting for HIPAA, PCI, and more
Multiplatform	Protects the full range of endpoints required by mobile and knowledge workers, including Macs, Linux, Windows, and mobile devices

McAfee

Supported Operating Platforms

Workstations

- Windows 7 or Embedded
- Windows Vista
- Windows XP Home, Professional, Embedded (WEPOS), Tablet PC
- Windows 2000 Professional with Service Pack 2 (SP2) or higher
- Mac OS X Snow Leopard (10.6), Mac OS X Leopard (10.5 or later), or Mac OS X Tiger (10.4.6 or later)

Servers

- Windows 2008 Server, Hyper-V, Core, Datacenter, Storage Server, Cluster Server, Small Business Server,
- Windows 2003 Server, Storage Server, Cluster Server, Datacenter, Small Business Server
- Windows 2000 Server, Advanced Server, Small Business Server
- Red Hat Linux, Novell Linux, SuSE Linux, Fedora, Ubuntu, CentOS
- VMware ESX, ESXi
- Citrix XenDesktop and XenServer

Other supported platforms

- FreeBSD 32-bit 6.1 and 7.0 (Command Line Scanner)
- HP-UX 11.0, 11i, 11i v2/v3 (Command Line Scanner)
- IBM AIX 5.2, 5.3, 6.1 (Command Line Scanner)
- Linux Kernel 2.4 (32-bit); 2.6 (64-bit) (Command Line Scanner)
- Solaris 8, 9, 10 (32-bit and 64-bit) (Command Line Scanner)
- Citrix MetaFrame 1.8 & XP Support
- EMC Celerra File Server

Email server requirements

- Microsoft Exchange 2003 SP1; 2007 (64-bit); 2010 (v7.0.2)
- Microsoft Exchange 2000 SMB, 2003 Server, or Advanced Server
- Lotus Domino 6.0.3-6.0.5; 7.0; 8.0 (32-bit); 8.5 (32-bit)

corporate network. Granular control includes content filtering and enforcement of website access by user and groups, with complete management and reporting.

Flexible network access control

Control access to corporate networks, enforce endpoint security policy, and integrate endpoint controls with existing network infrastructures. Regardless of how endpoints connect to the network, network access control discovers and evaluates endpoint compliance status, defines the appropriate network access policies, and provides automated remediation.

Always on, real-time malware protection

With the unprecedented growth of advanced persistent threats, enterprises cannot depend on solutions that rely solely on signature analysis for endpoint protection. There's a gap of 24 to 72 hours from the time a threat is identified to the moment its signature is applied to endpoints. In the meantime, your data and systems lie exposed. Built-in McAfee Global Threat Intelligence file reputation service closes the gap, providing real-time, always-on protection based on insight gathered by McAfee Labs™. By integrating research and response, McAfee can quarantine or block viruses, Trojans, worms, adware, spyware, and other potentially unwanted programs that steal confidential data and sabotage user productivity.

Learn More

For more information, visit www.mcafee.com/endpoint, or call us at 888.847.8766, 24 hours a day, seven days a week.

McAfee, Inc.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

14200ds_tops-e_0910_fnl_ASD